To print: **Click here** *or* Select **File** and then **Print** from your browser's menu

----
This story was printed from Inter@ctive Week,
located at http://www.zdnet.com/intweek.

Quantum Leaping

By *Sara Robinson*, Interactive Week
November 22, 2000 7:59 AM PT
URL:

Jonathan Dowling knew his research was interesting. he just didn't realize how interesting until government intelligence officials tracked him down.

The call came earlier this year after Dowling, a physicist at the National Aeronautics and Space Administration Jet Propulsion Laboratory in Pasadena, Calif., and his colleagues figured out a way to use quantum physical techniques to precisely synchronize two clocks.

After Dowling spoke with someone at the National Security Agency who expressed interest in the results, a member of his team jokingly sent out an e-mail suggesting that they auction off the results on eBay to the highest-bidding government. Amused, Dowling forwarded the e-mail to a friend at the NSA.

The very next day, a stranger at the National Reconnaissance Office, the shadowy branch of the Department of Defense (DOD) responsible for the government's surveillance activities, called and suggested funding Dowling's research because of its potential impact for spy satellite surveillance.

"It's an interesting gambit to tell the National Security Agency you have a secret and you're not going to tell it to them," Dowling chuckles, explaining that he didn't want to share the results until they were published. "We still don't know exactly what application they're interested in."

Dowling's experience illustrates the growing interest within the intelligence community in everything quantum. Quantum computing, quantum cryptography and now quantum clock synchronization are all futuristic technologies a long way from practical realization. Even so, they are becoming targets of significant amounts of defense- and intelligence-agency funding.

Quantum information theory, the broad heading under which all these topics fall, makes use of some of the weird physical properties exhibited by systems of very small particles. These properties, while difficult to harness in a practical way, enable new paradigms for storing, computing and protecting information.

"The new idea is that information is not just an abstract entity," says Umesh Vazirani, a professor of computer science at the University of California at Berkeley. "It is somehow embodied in the underlying quantum physics, and inherits some of its weird but powerful properties."

Quantum information theory first caught the eye of U.S. intelligence agencies six years ago, when AT&T

researcher Peter Shor demonstrated that a quantum computer could break the encryption codes that protect data transmissions over the Internet.

Because of the threat that Shor's algorithm poses to existing encryption techniques, there is also a great deal of interest in a possible antidote. Quantum cryptography, a way of using quantum techniques to securely transmit data, is a field that predates the current quantum hoopla. It has gained momentum as a way of filling the security hole that Shor's algorithm opened.

And now, quantum clock synchronization, a way to make two atomic clocks start ticking at once, is yet another application of quantum information theory that has attracted intelligence attention.

Dowling published his research on quantum clock synchronization in September; a group from IBM published similar results at the same time.

Meanwhile, the Defense Advanced Research Projects Agency, the main research funding arm of the DOD, recently allocated $100 million over five years to a program in Quantum Information Science and Technology (QuIST). This money, a small but significant bit of DARPA's $2 billion yearly budget, will fund research projects at universities, as well as government and corporate research labs.

In October, DARPA hosted a workshop in Washington, D.C., for scientists vying for the QuIST funding. In what workshop officials characterized as a "highly unusual" display of openness, various intelligence agencies within the DOD emphasized the importance of quantum information technology to national interests. Some agencies then went on to specify topics of particular interest.

One Step Ahead

During the workshop, Henry Everitt, of the army research office, noted that the U.S. maintains its technological edge by staying ahead of everyone else. Since Moore's law, which says that processor power roughly doubles every 18 months, will soon run into natural barriers, we must look to quantum technology to maintain our leading edge, he said. The NSA's Keith Miller and Dean Collins from Advanced Research and Development Activity in Information Technology, a newly formed funding agency for the DOD intelligence community, spoke of the importance of quantum computers – devices that use the properties of quantum physics to do computational tasks – and quantum cryptography. The NRO's Pete Hendrickson spoke of the new results in quantum clock synchronization and its possible uses for surveillance satellites.

An official representing the National Institute for Standards and Technology, the agency in charge of official technological standards, also expressed interest in quantum clock synchronization, since it could lead to new standards for measuring time.

Much of the research that has strategic importance to the government happens behind closed doors, conducted by researchers sworn to secrecy. Yet QuIST, like many of DARPA's basic research programs, will fund research that's freely publishable by its participants worldwide. Some of the researchers vying for QuIST funding are from universities in Canada and Europe.

This is because DARPA's explicit charter is not to carry out top-secret projects, but "to avoid technological surprises," says Shankar Sastry, DARPA's director of information technology. Indeed, Sastry says, the agency was created after the Russians launched Sputnik, an event that surprised and embarrassed the American intelligence community because no one had any inkling of the advanced state of the Russian space program.

By staying a part of the broader research community, DARPA can closely monitor the progress of research in various arenas and direct the attention of top researchers to problems of particular importance to the

DOD.

To further these goals, DARPA programs typically sponsor communities of researchers working on different aspects of a theme. These researchers are required to write regular progress reports and gather regularly for DARPA-sponsored conferences.

DARPA specifically aims to fund high-risk projects. Many projects of strategic importance might not capture the attention of other agencies, such as the National Science Foundation, that only use a peer-review process to allocate funds, as scientists are typically conservative about pursuing avenues that have only a small chance of success, Sastry says. DARPA uses an internal review as well as a peer review to evaluate research proposals.

Also, the NSF has far less money than DARPA, which tends to focus on a few, very expensive projects. "DARPA's general style is to pick a modest number of winners and get them big resources to hire personnel," Sastry says.

Quantum information theory certainly qualifies as high-risk research. The dramatic results are all theoretical. Most researchers agree that practical devices, if possible at all, are a long way off. Several groups of researchers have built tiny quantum computers that can store just a few bits, and have developed protocols for quantum cryptography that can send encryption keys over short distances. But it's not clear that any of the current approaches could lead to practical devices.

Still, the government has great hopes for the technology and is willing to dedicate vast resources toward addressing it. "Since the stakes are so high, it's worth it for us to make an investment," Sastry says. "The security of the entire Internet could be at risk."

Not surprisingly, intelligence officials say they'd like to see more research on quantum theory's potential to unlock existing codes and create new ones. More generally, DARPA officials say, they hope to find out more about what quantum computers can and cannot do.

A quantum computer stores information using the states of elementary particles as bits – the zeros and ones that are the basic units of information storage. For example, classically, the spin of an atomic nucleus can point either up or down. But when the mysterious workings of the quantum universe are taken into account, nuclear states are not just spin-up or spin-down, but a weighted combination of both simultaneously. As a result, quantum states seem to hover between two possible realities, an intriguing yet bizarre state of affairs.

What really intrigues scientists is that as the number of quantum bits grows, the amount of information required to describe the system grows exponentially. If each atomic nucleus is in one of two states, then, classically, a system of 500 nuclei will be in one of 2^{500} possible states. Quantum theory, however, says that the system at any moment is in a superposition of all of those 2^{500} possibilities at once, a system far more complex than any conceivable classical system.

Since 2^{500} is a huge number, far larger than the estimated number of particles in the universe, scientists question how the universe can manage to even keep track of its own natural processes. But the fact that it can hints at an enormous resource for storing information.

Still, for most tasks, quantum computers are not known to be more powerful than classical ones. Only in a few cases have researchers been able to devise special algorithms that make use of quantum properties to exponentially speed up certain computations. One example is Shor's algorithm for finding the prime factors of large numbers, a task that would take years on existing computers, but could be done in minutes with a quantum computer. The security of many encryption codes relies on the difficulty of factoring large numbers.

For now, however, Shor's algorithm is the only quantum algorithm of practical importance. But DARPA officials at the QuIST workshop say they would like to fund projects to look for more quantum algorithms or determine the limits of quantum computing power. None of the quantum computers that have been built to date can be scaled to a practical-size device.

Spotting Spies

Quantum cryptography, like quantum computing, uses techniques from quantum physics – in this case to securely transmit information along fiber-optic cables or through the air. But it exploits a different law of quantum physics: It's impossible to "look" at a quantum system without changing it in the process, so when secret information is sent by quantum methods, it's easy to detect eavesdroppers. This possibility of detecting whether information has been intercepted is intriguing to the NSA.

Quantum cryptographic signals can now be sent over fiber-optic cables and through the air for tens of miles; techniques are needed, however, to boost these signals without disturbing them and making it look as though someone has listened in.

Quantum clock synchronization – a way to make two atomic clocks set far apart start ticking at once – uses similar techniques to those used in quantum cryptography.

The NRO suggested that clock synchronization has uses in spy satellites, but didn't give any more specifics. Dowling, however, speculated that the technique would be useful for calibrating signals from two different spy satellites and for global positioning systems.

Spy satellites bounce light waves off objects to gather intelligence about the objects. Typically, two satellites will send light from different angles. When the signals bounce back to the satellite, one signal is subtracted from the other and the difference gives detailed information about the makeup of the object. In order to use this technique accurately, however, beams of light from the two different satellites have to be synchronized.

Similarly, global positioning systems pinpoint a location by sending information from two different satellites some distance apart. Current clock synchronization techniques for these systems can lead to errors of up to several meters.

Another potentially significant application of clock synchronization, Sastry says, is to enable fast routing of data over the Internet. Currently, data carried as light waves over fiber-optic channels must be translated into slower electronic signals. But as we move to an all-optical Internet, where the amount of data passing through a router is much larger, router clocks will have to be more precisely synchronized.

While all these applications have yet to be embodied in practical devices, they show that quantum theory has the potential to change the way we process information. Viewed in this manner, it's not surprising that the information-gathering intelligence agencies think it's worth a substantial investment.